Advisory
Title: Potential Internet Attack Targeting Microsoft Beginning August 16, 2003
Date: August 14, 2003

OVERVIEW

The National Cyber Security Division (NCSD) of the DHS / Information Analysis and Infrastructure Protection Directorate is issuing this advisory to heighten awareness of potential Internet disruptions beginning August 16, 2003. An Internet worm dubbed "msblast", "lovesan", or "blaster" began spreading on August 11th that takes advantage of a recently announced vulnerability in computers running some versions of the Microsoft Windows operating system. DHS addressed this issue in an advisory available at **http://www.dhs.gov/interweb/assetlibrary/Advisory_Internet_Impact_MS2.PDF**. NCSD would like to highlight that this worm contains additional code which may cause infected computers to attempt repetitive connections to a popular Microsoft web site, **www.windowsupdate.com** beginning just after midnight on the morning of August 16th.

IMPACT

Because of the significant percentage of infected computers using high speed connections to the Internet (DSL or cable for example) the conditions exist for a phenomena known as a distributed denial of service (DDoS) attack against the Microsoft web site beginning on August 16th. Steps are being taken by Microsoft and by Internet Service Providers to mitigate the impact of the DDoS. Owners of computers infected by the worm may experience a general slowness of their computer along with difficulty in connecting to Internet sites or local network resources. Systems that are still infected on August 16th may stop spreading the worm and may begin flooding the Microsoft Update site with repeated connection requests. Other customers who attempt to use the site to update their Microsoft Windows operating systems on or after August 16th might experience slowness in response or inability to connect to the update site.

DETAILS

Windowsupdate.com is used as a starting point for users of Microsoft Windows operating systems for software updates. The code in the worm instructs infected computers to repeatedly connect to that site beginning on the 16th of August. Starting on January 1, 2004, the worm will switch to cyclic behavior in which it attacks the Microsoft web site from the 16th of each month to the end of the month. Between the 1st and 15th of the month, infected computers may attempt to scan for other vulnerable systems in order to spread the worm. The worm uses the clock in the infected computer to determine when to start and stop; therefore Microsoft may begin seeing attacks on the morning of the 15th due to time zone differences around the world. This pattern of spreading from the 1st to the 15th and flooding Microsoft between the 16th and the end of the month may continue indefinitely.

RECOMMENDATIONS

The worm takes advantage of a serious vulnerability in several versions of the Microsoft Windows operating system. DHS encourages system administrators and computer owners to update vulnerable versions of Microsoft Windows operating systems as soon as possible before August 15th.

Details on which computers are vulnerable and instructions for cleaning infected computers are available at
http://www.microsoft.com/security/incident/blast.asp.

DHS also encourages system administrators and computer owners to update antivirus software with the latest signatures available from their respective software vendor.

In order to limit the spreading of the worm, DHS further suggests that Internet Service Providers and network administrators consider blocking TCP and UDP ports 69, 135, 139, 445, and 4444 for inbound connections unless absolutely needed for business or operational purposes.

DHS encourages recipients of this Advisory to report information concerning suspicious or criminal activity to local law enforcement, local FBI's Joint Terrorism Task Force or the Homeland Security Operations Center (HSOC). The HSOC may be contacted at: Phone: (202) 282-8101.

DHS intends to update this advisory should it receive additional relevant information, including information provided to it by the user community. Based on this notification, no change to the Homeland Security Advisory System (HSAS) level is anticipated; the current HSAS level is YELLOW.